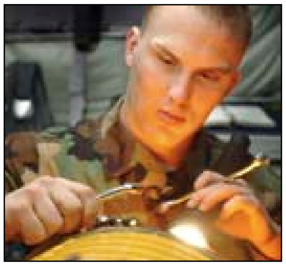


U.S. EUROPEAN COMMAND

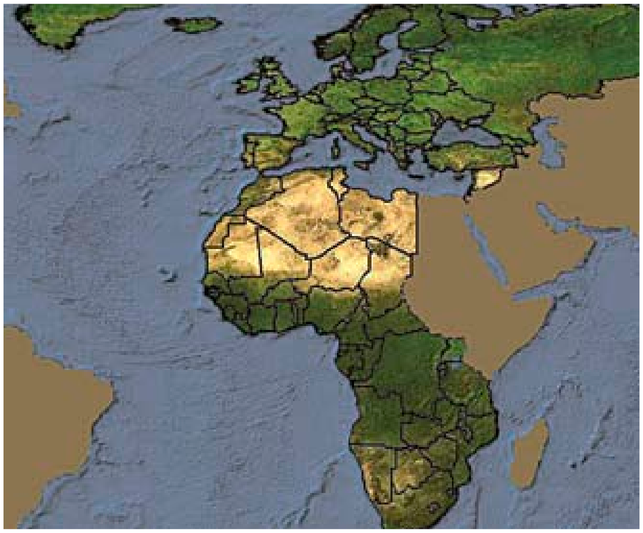
Host Commander Site

U.S. European Command (USEUCOM) is the unified combatant command charged with defending and advancing U.S. national interests in a 91-country area of responsibility spanning from the North Atlantic, across Europe and Russia to South Africa. Diverse is the word which best describes USEUCOM's theater, which includes many of the world's richest and poorest nations. The command maintains ready forces to conduct the full range of operations, unilaterally or in concert with coalition partners, to promote regional stability, counter terrorism and enhance transatlantic security through support of NATO.

USEUCOM is transforming its base and force structure to become more agile, expeditionary, capable and interoperable – all essential to meeting the challenges of today's complex security environment. The command strategy emphasizes preventive, "Phase 0" theater security cooperation. This approach seeks partnerships to enhance regional security capabilities in developing nations, denies safe haven for terrorists and deals with underlying causes of conflict. Building on the strength of a transformed NATO alliance and working with key countries and regional organizations in Africa, Eastern Europe and the Caucasus are key elements of this strategy.

Equally important is establishing command and control structures and processes that take advantage of new technologies, leverage the capabilities of the Interagency Community, and enable faster, flexible planning and execution with effects-based solutions. Coalition interoperability is absolutely critical if we are to rapidly respond to events that may occur with little or no warning. This year's Coalition Warrior Interoperability Demonstration (CWID) will help close the gaps by evaluating trial technologies that demonstrate warfighter utility and can be fielded within 12-18 months.

This year's demonstrations will be hosted at Kelley Barracks in Stuttgart, Germany, from May 30 until June 23, 2006.



TRANSPORTATION INFORMATION AND DIRECTIONS

FROM THE STUTTGART AIRPORT TO KELLEY BARRACKS

■ **A taxi from the airport** to Kelley Barracks is about 15 Euros ($18). Although some taxis will take credit cards, the best bet is to use the airport ATM or currency exchange before leaving the airport so you can pay in cash. Drivers provide receipts upon request. Tipping the driver is not necessary but is appreciated. If you do tip, 1-2 Euros is sufficient.

■ **Driving from airport exit,** turn left. Stay in the right lane looking for Route 27 towards Stuttgart, approximately .5 miles. Stay in right lane to get on Route 27 and then move to the center lane.

■ Once you have passed the exit for A8, stay to the right for about 1.5 miles. You will go one more exit before getting off. Follow signs for Kelley Barracks. Keep right and make the right hand turn, then change to the left lane. Pass the first light and turn left at the second light.

■ Stay to the left after making the turn. Kelley Barracks starts right after the Daimler-Chrysler complex.

■ The gate guard will ask to see your identification (passport or ID card) before permitting you access to the base.

SCHEDULE OF EVENTS

May 30-June 23: Execution

■ **May 30-June 4:** National Integration/Final Testing and Trial Set-Up

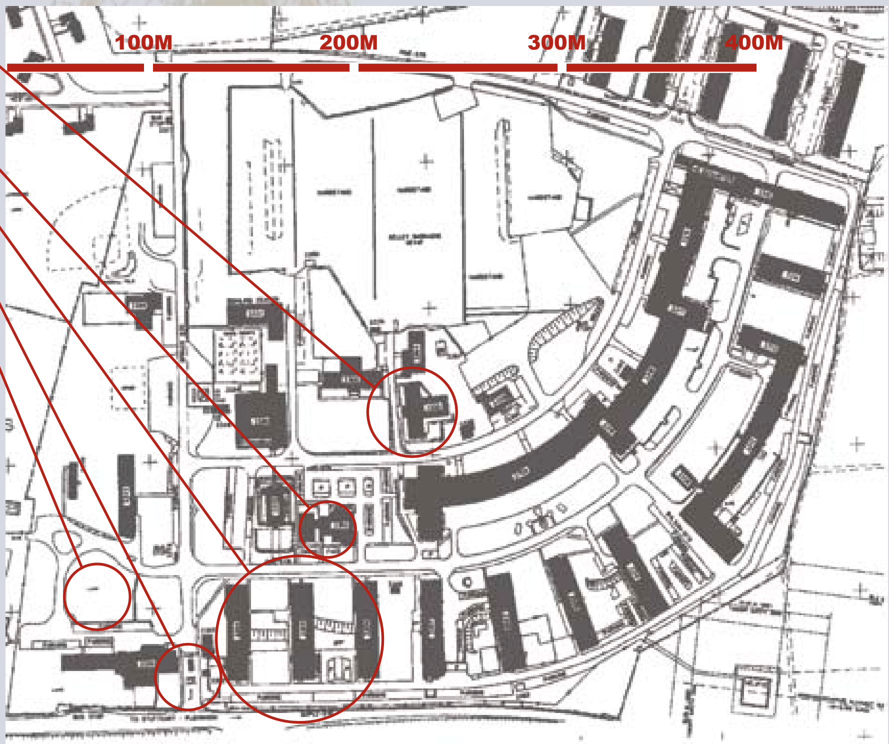
■ **June 5-11:** Coalition Integration, Scenario Training and Rehearsal

■ **June 12-22:** Execution and Assessment

■ **June 19-22:** Visitor Week

■ **June 23:** Hot Wash

STUTTGART



VISITOR CLEARANCES

Clearances are due to SrA Phillips prior to your visit. Badges will be issued for entry/exit to Kelley Barracks and the CWID work site. Please contact CW04 Kent Schneider or IT1 Mark Nunn to ensure you are listed as visitor for your initial entry to the post.

POINTS OF CONTACT

e-mail: cwid@eucom.mil

Maj Teri Centner
CML +49-711-680-4383
DSN 314-430-4383

LCDR Ian Branum
CML +49-711-680-4895
DSN 314-430-4895

CW04 Kent Schneider
CML +49-711-680-7094
DSN 314-430-7094

IT1 Mark Nunn
CML +49-711-680-4364
DSN 314-430-4364

SrA Michelle Phillips
CML +49-711-680-8705
DSN 314-430-4364
phillpm@eucom.mil

LT Nancy Harrity
+49-711-680-7108
DSN 314-430-7108
harrityn@eucom.mil

OTHER PHONE NUMBERS

Kelley Hotel
CML +49 (0)711-729-2815/2304/
DSN 314-421- 2815/2304

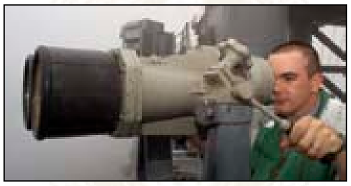
USO
CML +49 (0)711-680-5559/DSN
314-430-5559

SI Centrum/Millenium CML +49 (0)711-721-0 (hotel and entertainment complex)

Enjoy Tours
CML +49(0)6301-6000
www.enjoytours.com

Trials at USEUCOM CWID Operations Building

IT01.15	C4I DEFENSE
IT01.50	MULTINATIONAL INTEROPERABILITY TOOLKIT (MIT)
IT01.53	COALITION AND CIVIL AGENCY CAPABLE WIRELESS INFORMATION TRANSFER SYSTEM (C3WITS)
IT03.09	DOCUMENT ACCESS SERVLET (DAS)
IT03.16	INTELLIGENT ROAD/RAIL INFORMATION SERVER (IRRIS)
IT04.33	LOGIK V3.0 FOR RAPID INTELLIGENCE ANALYSIS AND EXPLOITATION
IT05.17	WMD COLLABORATIVE ADVISORY RESPONSE SYSTEM
IT05.32	GUARD NET PORTAL (GNP)
IT05.37	JOINT EFFECTS BASED COMMAND AND CONTROL (JEBC2)
IT05.51	FORCENET DISTRIBUTED CHANNEL SERVICES (FNDCS) INFORMATION MANAGER
IT05.66	COALITION SHARED INFORMATION NETWORK ENVIRONMENT (COSINE)



NORTH AMERICAN AEROSPACE DEFENSE-U.S. NORTHERN COMMAND

Site for Homeland Security and Homeland Defense

NORAD-USNORTHCOM, Colorado Springs, Colo., employs CWID to forge new coalitions. Traditional CWID participation expands this year to involve partners in other government agencies that would be part of any emergency response effort.

Future coalitions will be created on the fly, based on events. It will benefit all potential contributors, international and domestic, to be familiar with the military information environment. Many information technologies, along with associated tactics, techniques and procedures to support response efforts, will be evaluated during CWID 2006.

Trials at NORAD-USNORTHCOM will focus on the Homeland Defense mission, demonstrating technological advances in information sharing, collaboration, wireless technologies and web-based situational awareness tools.

CONTACTS

Chris Lambert, Program Manager
719.554.8064
DSN: 692.8064

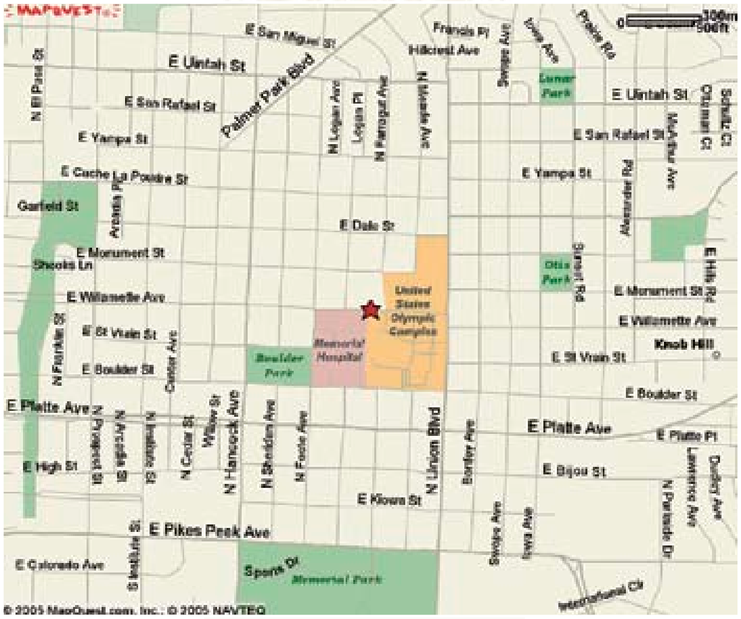
Marie Miller, Site Manager
719.554.2802
DSN: 692.2802

Dan McCarthy, Scenario Lead
719.554.4423

Catherine Jackson, Network Engineer
719.554.7424

CWID demonstrations will be hosted at the Federal Building, 1520 E. Willamette, Colorado Springs, Colo., during the execution phase 12 to 22 June 2006.

Colorado Springs is the second largest city in the state with a population of approximately 500,000. Colorado Springs hosts the United States Air Force Academy to the north, Peterson Air Force Base to the east, Fort Carson to the south and Schreiver AFB to the east. Peterson AFB is home to NORAD-USNORTHCOM. The Federal Building, the CWID 2006 site in the city of Colorado Springs, is an off-base facility. The Colorado Springs Airport, which shares runways with Peterson AFB, services the area with direct connections to many major travel hubs.



FROM THE AIRPORT

Exit the airport via Drennan Road, go west to Powers Blvd.; go north on Powers Blvd to Platte Ave.; go west on Platte Ave. to Boulder; go west on Boulder to Hancock; go north on Hancock to Willamette; go east to 1520 E. Willamette.

PUBLIC AFFAIRS CONTACT
William Ford
719.554.1089
NORAD-USNORTHCOM

CWID Trials at NORAD-USNORTHCOM

IT01.34	Mobile / Static Real-Time Radiological Surveillance Network (MobRadNet)
IT01.39	FIRST Responder INTERoperable COMMunications (First InterComm™)
IT01.48	Emergency Response Coalition - Common Operating Picture
IT01.53	Coalition and Civil Agency Capable Wireless Information Transfer System (C3WITS)
IT01.54	Coast Guard C2 (Deepwater COP) (CG-C2)
IT01.63	IPC Information Systems, LLC Multimedia Command and Control Solution (MCCS)
IT02.45	Command Center Portal Framework (CCPF)
IT03.09	Document Access Servelet (DAS)
IT03.16	Intelligent Road/Rail Information Server (IRRIS)
IT04.03	Wide Area Interoperability System (WAIS) and ACU-1000
IT04.33	Logik v3.0 for Rapid Intelligence Analysis and Exploitation
IT04.36	Global Broadcast Service (GBS)
IT04.46	Joint C4 Coordination Support System (JCCSS)
IT05.17	WMD Collaborative Advisory Response System (WMDCARS)
IT05.32	Guard Net Portal (GNP)
IT05.37	Joint Effects Based Command and Control (JEBC2)
IT05.47	HLS-HLD Collaborative Information Exchange Environment (HLS-HLD CIEE)
IT05.51	FORCEnet Distributed Channel Services (FnDCS)
IT05.52	Rapid Triage Medical Workbench (RTMW)

U.S. MARINE CORPS SITE, DAHLGREN, VA.

Naval Surface Warfare Center

The U.S. Marine Corps, U.S. Army, U.S. Coast Guard and National Guard have selected NSWC Dahlgren Division, Dahlgren, Va., as their primary CWID 2006 site, including coalition land component commander (CFLCC) operations.

The Naval Surface Warfare Center Dahlgren Division (NSWCDD), a key contributor to the NAVSEA Warfare Centers team, consists of three sites: Dahlgren Laboratory, the Combat Direction Systems Activity Dam Neck, Va., and Coastal Systems Station Panama City, Fla.

This year Dahlgren has the privilege to host the Coalition Force Land Component Commander (CFLCC), and three additional simulated afloat and ashore Command Centers. In addition, Dahlgren will participate in the emerging Homeland Defense/Homeland Security initiatives led by the National Guard Bureau with support from the U.S. Coast Guard, U.S. Navy and U.S. Marines.

Under leadership of CAPT Joseph McGettigan, USN, Commander NSWCDD, the warfare center's primary mission is to deliver solutions to the warfighter while continuing to build the Navies of the future in the most effective and efficient manner. Dahlgren Division's unique capability to understand and anticipate warfighter needs is a result of the continued professional growth and development of its workforce to sustain authority in the field. If the science and technology to meet warfighter needs doesn't exist, the division has the ability to create and accelerate new technology into an affordable capability to the warfighter.

The Naval Sea Systems Command's ongoing realignment of its warfare centers (both surface and underwater) continues in 2006 with the goal to build technical capacity across warfare centers, that can be harnessed without redundancy by Product Area Directors as identified by NAVSEA, to deliver products that meet Navy requirements of Sea Power 21.

NSWC DAHLGREN DIVISION WEB SITE
http://www.nswc.navy.mil

SITE MANAGER
Bill Ormsby
540.653.8209
FAX: 540.653.0040
william.f.ormsby@navy.mil

PROTOCOL CONTACT
Kathleen Rector
540.284.0870
FAX: 540.653.4679
kathleen.rector@navy.mil

MEDIA CONTACT
John Joyce
540.653.0365
FAX: 540.653.4679
john.j.joyce2.ctr@navy.mil

ALTERNATIVE PROTOCOL/ MEDIA CONTACT
Stacia Courtney
540.653.8154
stacia.courtney@navy.mil

To that end, the Underwater and Surface Warfare centers were aligned into 12 Product Areas (PAs). Dahlgren Division is directly involved in building technical capacity across all three sites with six of those Product Areas: Surface Ship Combat Systems; Navy Strategic Weapon Systems; Ordnance; Littoral Warfare Systems; Homeland Force Protection; and Force Level Warfare Systems.

NSWCDD is uniquely positioned to help navigate the road to transformation. Its broad spectrum of resources, including workforce, infrastructure, and relationships with industry, have already made it a premier naval scientific and engineering institution that is dedicated to solving a diverse set of complex technical problems confronting the warfighter, whether on land, in the air, on the sea or in space.

Across its three sites, Dahlgren Division spent years building, testing, and stretching a technical infrastructure that is simply not available elsewhere. The division exists to understand technical dimensions of military problems, to know who can provide technical solutions to these problems and to know whether a responsible solution has been provided. This is accomplished by addressing three attributes of navy ownership: unimpeded access to intellectual facilities and resources, connectivity between the warfighter and the technical community, and a continuous source of competence to ensure integrity over the entire life cycle of a system. It can not be done alone; it requires sustained relationships with the warfighter, sponsors, industry and academia.

SECURITY

Val (Lucas) Shepherd
Valencia.Lucas@navy.mil
FAX: 540.653.6957

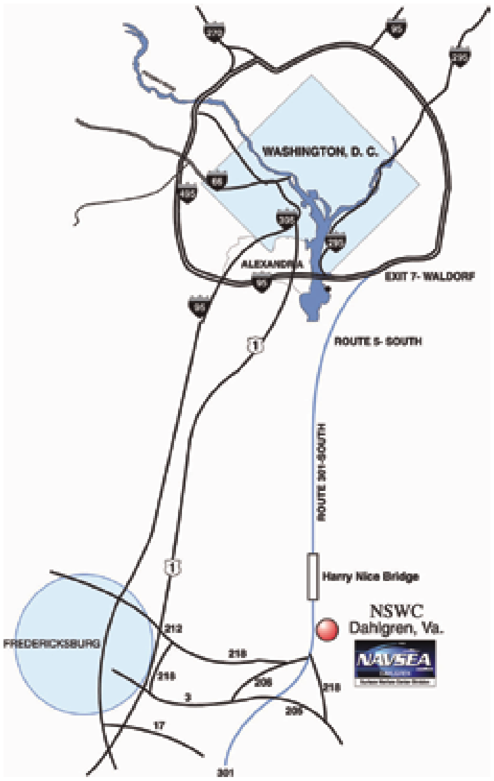
Voice confirmation:
540.653.5479

All security clearance information should be faxed to the security fax number.

FOREIGN REQUESTS

Brenda Bennett
540.653.3682
FAX: 540.653.4372
brenda.bennett@navy.mil

Barnita Byrd
540.653.8721
bamita.byrd@navy.mil



CWID Trials at NSWC Dahlgren Division

IT01.14	U.S. Chemical Biological Radiological and Nuclear Modeling (USCBRNM)
IT01.15	C4I Defence
IT01.20	Integrated Information Management System
IT01.34	Mobile/Static Real-Time Radiological Surveillance Network (MobRadNet)
IT01.48	Emergency Response Coalition - Common Operating Picture
IT01.53	Coalition and Civil Agency Capable Wireless Information Transfer System (C3WITS)
IT01.54	Coast Guard C2 (Deepwater COP) (CG-C2)
IT01.62	MobileForcesSolution (MOFS/MCCIS)
IT01.63	Multimedia Command and Control Solution (MCCS)
IT02.21	The Multi National Coalition Security System (MNCSS)
IT02.25	Distributed Common Ground System (DCGS)
IT03.09	Document Access Servelet (DAS)
IT03.16	Intelligent Road/Rail Information Server (IRRIS)
IT04.33	Logik v3.0 for Rapid Intelligence Analysis and Exploitation
IT04.36	Global Broadcast Service (GBS)
IT04.46	Joint C4 Coordination Support System (JCCSS)
IT05.06	Visualization for Information Assurance (VIA)
IT05.32	Guard Net Portal (GNP)
IT05.47	HLS/HLD Collaborative Information Exchange Environment (HLS-HLD CIEE)
IT05.51	FORCEnet Distributed Channel Services (FnDCS)
IT05.52	Rapid Triage Medical Workbench (RTMW)

U.S. ARMY AT DAHLGREN

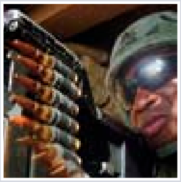
The Ground Combat View

The Army is collocated with the U.S. Marine Corps at NSWC Dahlgren, Va. The Army's assists U.S. entities and the international community with investigation of command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) technologies and interoperability solutions for near-term interagency, joint and coalition interoperability challenges. The Army will achieve this role during CWID 2006 by evaluating C4ISR Interoperability Trials in the conventional arena and the Homeland Defense/Security arena by commanding the Tactical Operations Center.

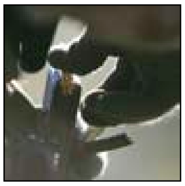
CONTACT

John Saputo
HQDA G6
703 602 7364
john.saputo@hqda.army.mil

GOALS FOR 2006



- Provide relevant and ready landpower for the 21st century security environment
- Train and equip Soldiers to serve as warriors and growing adaptive leaders
- Sustain an All-Volunteer force composed of highly competent Soldiers that are provided an equally high quality of life
- Provide infrastructure and support to enable the force to fulfill its strategic roles and missions
- Improve the technology necessary to provide the leadership, decision making, and integration of Army Forces with other joint forces, multinational forces, coalition forces, and interagency elements to conduct dominant maneuver, necessary situational awareness and intelligence, focused logistics, precision fires, and full dimensional protection
- Link CWID to the Army's overall experimentation efforts, inserting information technology from the foxhole to the industrial base



U.S. MARINE CORPS AT DAHLGREN

Leveraging Tech Programs

The United States Marine Corps looks forward to the opportunity to participate and evaluate Interoperability Trials that will support warfighters and first responders in the Coalition Warrior Interoperability Demonstration (CWID) 2006.

The U.S. Marine Corps recognizes the importance of evaluating the CWID Interoperability Trials (IT). It will allow warfighters immediate enhancements to interoperability solutions with Coalition and Joint Forces, United States Federal Agencies and Bureaus.

The Marine Corps is extremely qualified to participate and evaluate the CWID 2006 IT trials, because of the Marine Corps flexibility in conducting coalition and joint warfare, as well as supporting the Department of Homeland Security (DHS), the Federal Emergency Management Agency (FEMA), and the U.S. Northern Command's (NORTHCOM) in Homeland Security (HLS) and Homeland Defense (HLD) missions. The Marine Corps demonstrated its flexibility this past year by supporting the coalition forces in Iraq and Afghanistan, which enhanced coalition, joint and allied operations. The Marine Corps also provided first responders in support of homeland contingencies during Hurricanes Katrina and Rita.

CWID 2006 will allow the Marine Corps to assess emerging interoperable technologies in the Coalition and Joint operations arenas, as well as the HLS/HLD arenas through cooperation with allied partners and government agencies.

The Marine Corps expects nothing less than outstanding results from the assessment of IT trials that will support Marine Corps operating forces whether working on the battlefield against terrorists or as first responders in disaster relief operations, while working with the various Coalition and Joint Forces, Federal Agencies and Bureaus. This worldwide demonstration will provide dynamic new technologies, which will strengthen the warfighter's and first responders' abilities, and satisfy the Joint Staff, Combatant Commands, Agencies, Bureaus and Services' goals.

MARINE CORPS C4ISR GOALS

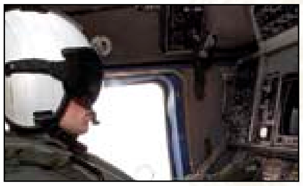
Build the Network, which includes to develop future USMC IT infrastructure, develop the Marine Corps Enterprise Network, expand the USMC Expeditionary C4 capabilities, acquire integrated systems, provide C4 guidance for C2 platform development, implement a USMC IT capital planning process, develop IT policies and standards, and to establish governance over the network.

Man the Network, which includes to enhance the health of the C4 occupational field, and to ensure the C4 training and education satisfies the Marine Corps mission requirements.

Populate the Network, which includes to evaluate existing technologies (such as portals collaboration tools, document and task management systems, and other web-based technologies), evaluate and identify new technologies to assist in problem solving, improve effectiveness, and promote efficiency, conduct business and technical analyses on proposed enterprises solutions to ensure that the network will be populated with those tools, applications, and systems that offer the greatest benefits to the Marine Corps, deploy IT solutions that provide analytical tools that leverage authoritative data sources fed by the data owners, and instantiate the USMC software baseline and application rationalization processes to ensure Marine Corps applications are interoperable with the network-centric views of Transformational Communications, GIG-BE, and USMC enterprise.

Protect the Network, which includes to provide computer network defense, and to provide computer emergency response.

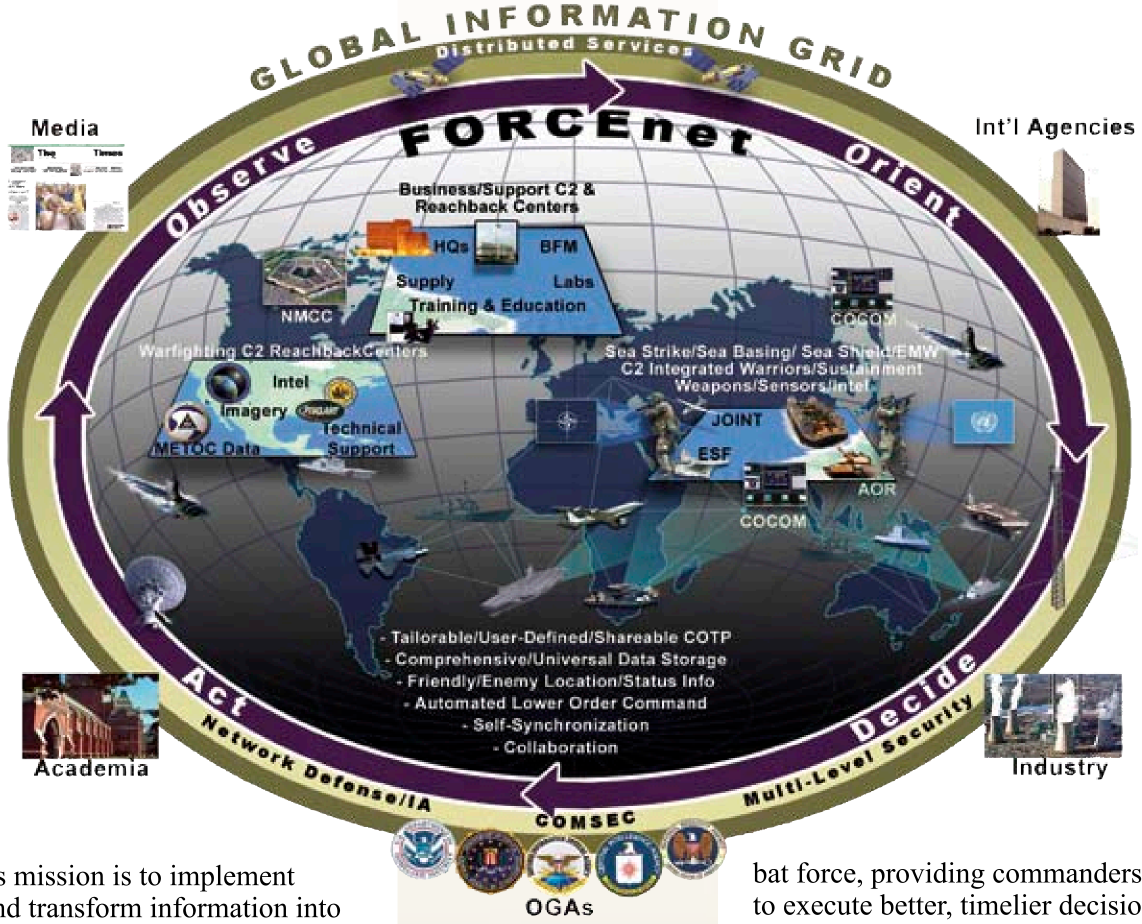
Exploit the Network, which will allow the Marine Air Ground Task Forces, joint, naval, and multinational (coalition) network operations, provide strategic agility (allowing rapid transition from a pre-crisis state to a full operational capability in a distant theater), provide operational reach to allow the projection and sustainment of relevant and effective power across the depth of the battle space, provide tactical flexibility by supporting multiple, concurrent, and dissimilar missions, and employ an agile supporting establishment.



U.S. NAVY SITE, SAN DIEGO, CALIF.

Space and Naval Warfare Systems Command

Rear Admiral Michael C. Bachmann, Commander, Space and Naval Warfare Systems Command (SPAWAR), hosts the U.S. Navy's site. SPAWAR's Office of the Chief Engineer designs the architecture and standards for FORCEnet, the Navy's vision for network-centric warfare and a key element of the Sea Power 21 philosophy.



SPAWAR's mission is to implement FORCEnet and transform information into decisive effects for the joint warfighter. In this spirit, SPAWAR welcomes the CWID U.S. and Coalition Interoperability Trials and all stakeholders in the development, acquisition, and fielding of critical information technologies. FORCEnet integrates warriors, sensors, command and control, platforms, and weapons into a networked combat force, providing commanders the means to execute better, timelier decisions. But FORCEnet is more than a warfighting system; it also encompasses business strategies through the acquisition of C4I, surveillance, reconnaissance, information technology and space systems. Ultimately, FORCEnet will significantly enhance knowledge superiority by allowing Navy and Marine Corps elements to link with joint, allied and coali-

CWID'S U.S. NAVY SITE IS LOCATED AT SPAWAR IN SAN DIEGO, CALIF.

The SPAWAR CWID Team assembles an actual joint and coalition battle staff; matching Coalition Interoperability Trial requirements to requested support from U.S. Navy, U.S. Marine Corps, U.S. Coast Guard, National Guard, and Coalition Navy sources.

For the CWID 2006 execution scenario, SPAWAR is also home to the Combined Forces Maritime Component Commander (CFMCC) and U.S. Coast Guard Joint Harbor Operations Center (JHOC).

VISIT REQUEST ADDRESS

SPAWARSYSCEN, SAN DIEGO
Attn: Visitor Control OTC
53560 Hull Street
San Diego, CA 92152-5001

FAX: 619.524.2745
619.524.2751 or 3124
(for verification)

PERSONS TO BE VISITED

CDR Doug Blackburn
SPAWAR Code 051E
619.524.7714

Ron Anderson
SSC-SD Code 2644
858.537.0204

INTERNATIONAL VISITOR CONTACT

FOREIGN VISITS OFFICE

Patti Talley
patti.talley@navy.mil

foreign@spawar.navy.mil
619.524.2398
FAX: 858.537.0127

POC FOR VISIT

Ron Anderson SSC-SD
Code 2644
858.537.0204
FAX: 858.537.0153

tion forces through seamless interoperability within the Defense Department's Global Information Grid (GIG). Accomplishing this essential mission requires a considerable degree of cooperation with diverse stakeholders. By partnering with Naval Operations Command for resources and Naval Network Warfare Command to identify FORCEnet requirements, SPAWAR designs, develops and delivers FORCEnet products by leveraging technical and administrative expertise within the TEAM SPAWAR workforce. The TEAM SPAWAR is composed of several organizations and program executive offices (PEOs) that are dedicated to transformational capabilities. They include:

- SPAWAR Headquarters (San Diego)
- PEO C4I and Space (San Diego)
- PEO Space Systems (Chantilly, Va.)
- PEO Enterprise Information Systems

TEAM SPAWAR lays the foundation for dramatic increases in a new era of warfighting capabilities and future readiness.

SPAWAR is located in San Diego's Old Town just west of Interstate 5 at 4297 Pacific Highway. Exit "Old Town" from 5 South, or exit "Pacific Highway" from 5 North.

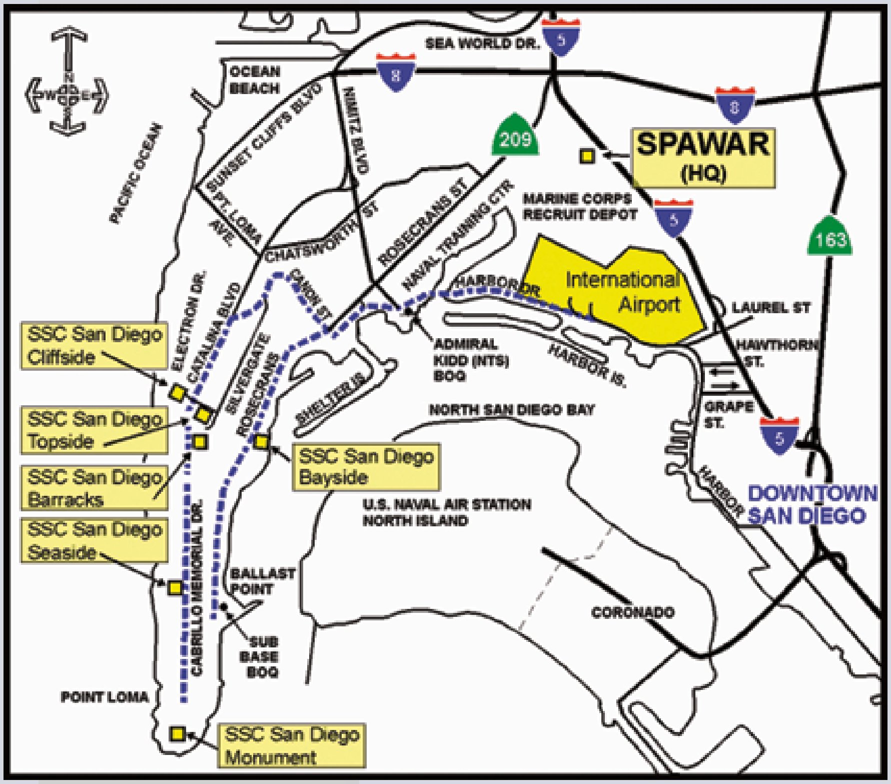
VISITOR'S RECEPTION is located just north of the pedestrian bridge. The CWID site is located in Building OT-3, 2nd Floor, East Mezzanine, Rooms 2430, 2434, 2438.

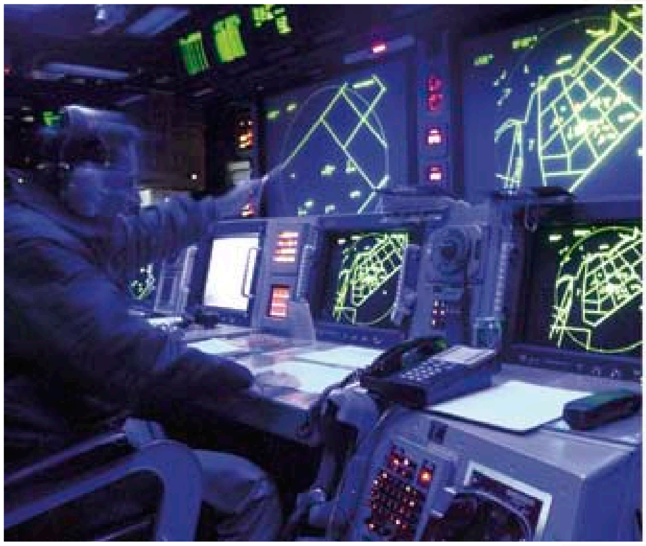
VISITOR INFORMATION

http://enterprise.spawar.navy.mil

- Select "Field Activites/San Diego"

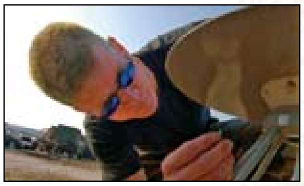
(Visitor Requests, Access, and Parking)





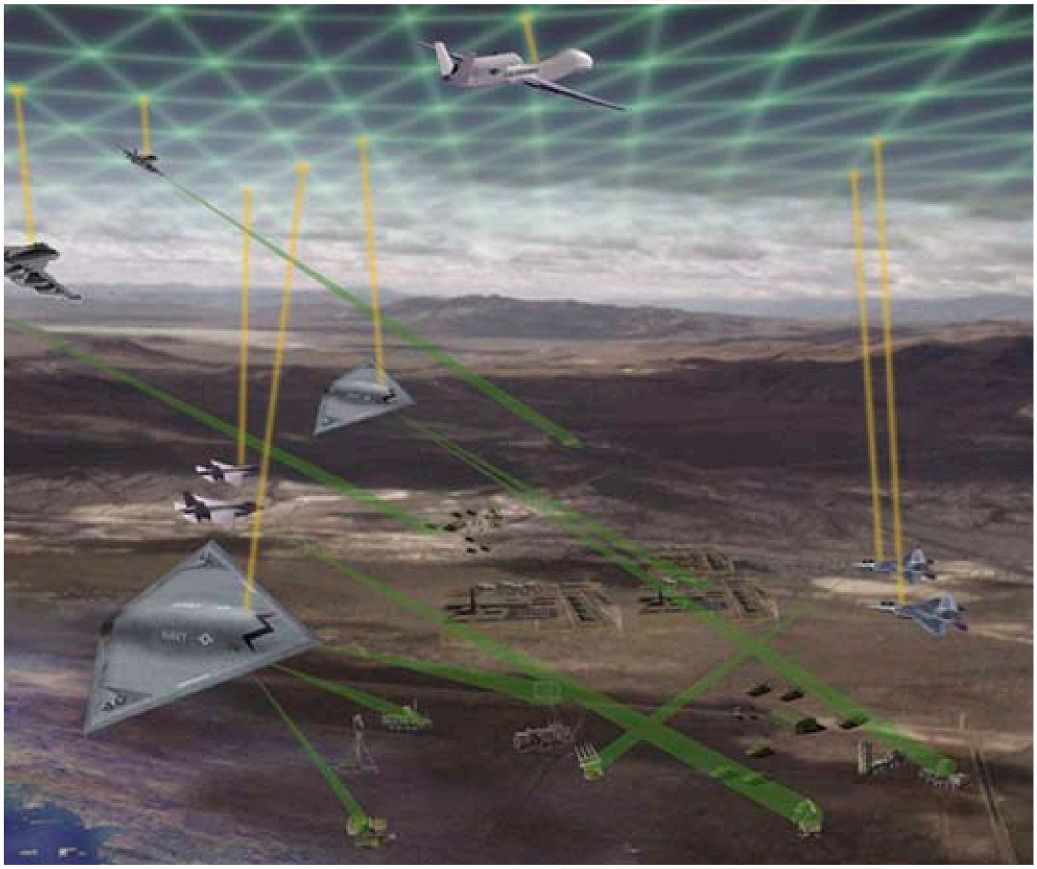
CWID Trials at SPAWAR

IT01.15	C4I Defense
IT01.20	Integrated Information Management System
IT01.34	Mobile / Static Real-Time Radiological Surveillance Network (MobRadNet)
IT01.50	Multinational Interoperability Toolkit (MIT)
IT01.53	Coalition and Civil Agency Capable Wireless Information Transfer System (C3WITS)
IT01.54	Coast Guard C2 (Deepwater COP) (CG-C2)
IT01.62	MobileForcesSolution (MOFS / MCCIS)
IT02.21	The Multi National Coalition Security System (MNCSS)
IT02.25	Distributed Common Ground System (DCGS)
IT03.09	Document Access Servelet (DAS)
IT03.16	Intelligent Road/Rail Information Server (IRRIS)
IT04.33	Logik v3.0 for Rapid Intelligence Analysis and Exploitation
IT04.61	MCCIS-I
IT05.32	Guard Net Portal (GNP)
IT05.37	Joint Effects Based Command and Control (JEBC2)
IT05.51	FORCEnet Distributed Channel Services (FnDCS)
IT05.52	Rapid Triage Medical Workbench (RTMW)



U.S. AIR FORCE SITE, HANSCOM AIR FORCE BASE, MASS.

Electronic Systems Center



The outcome we must achieve: "...fundamentally joint, network-centric, distributed forces capable of rapid decision superiority and massed effects across the battlespace"

DONALD RUMSFELD
SECRETARY OF DEFENSE

Air Force Materiel Command's Electronic Systems Center (ESC) is Hanscom's host organization. Activated 1 April 1961, ESC manages the development and acquisition of electronic command, and control (C2) systems. These systems gather and analyze information on potentially hostile forces, enabling commanders to make quick decisions and rapidly pass them on to their forces. They help to direct the muscle of America's air-power arsenal to the right target at the right time.

With an annual budget of approximately $3 billion, ESC is the Air Force's leader in command and control programs. It manages nearly 200 programs, ranging from secure communication systems to mission planning systems. ESC is involved in many significant C2 programs around the world. ESC personnel are helping to upgrade the North American Aerospace Defense Command headquarters. ESC is developing security systems for the protection of Air Force weapon systems and installations. They are also working with the Federal Aviation Administration to install new radar displays and improve air traffic control at major airports. In addition to providing C4I systems to the U.S. military, ESC people are developing air defense systems for allied forces such as the Royal Thai and Royal Saudi Air forces and NATO partners.

In the future, ESC will continue as the U.S. Air Force's center for the development of command and control systems. In 2001 the Air Force gave ESC the lead responsibil-

CONTACTS

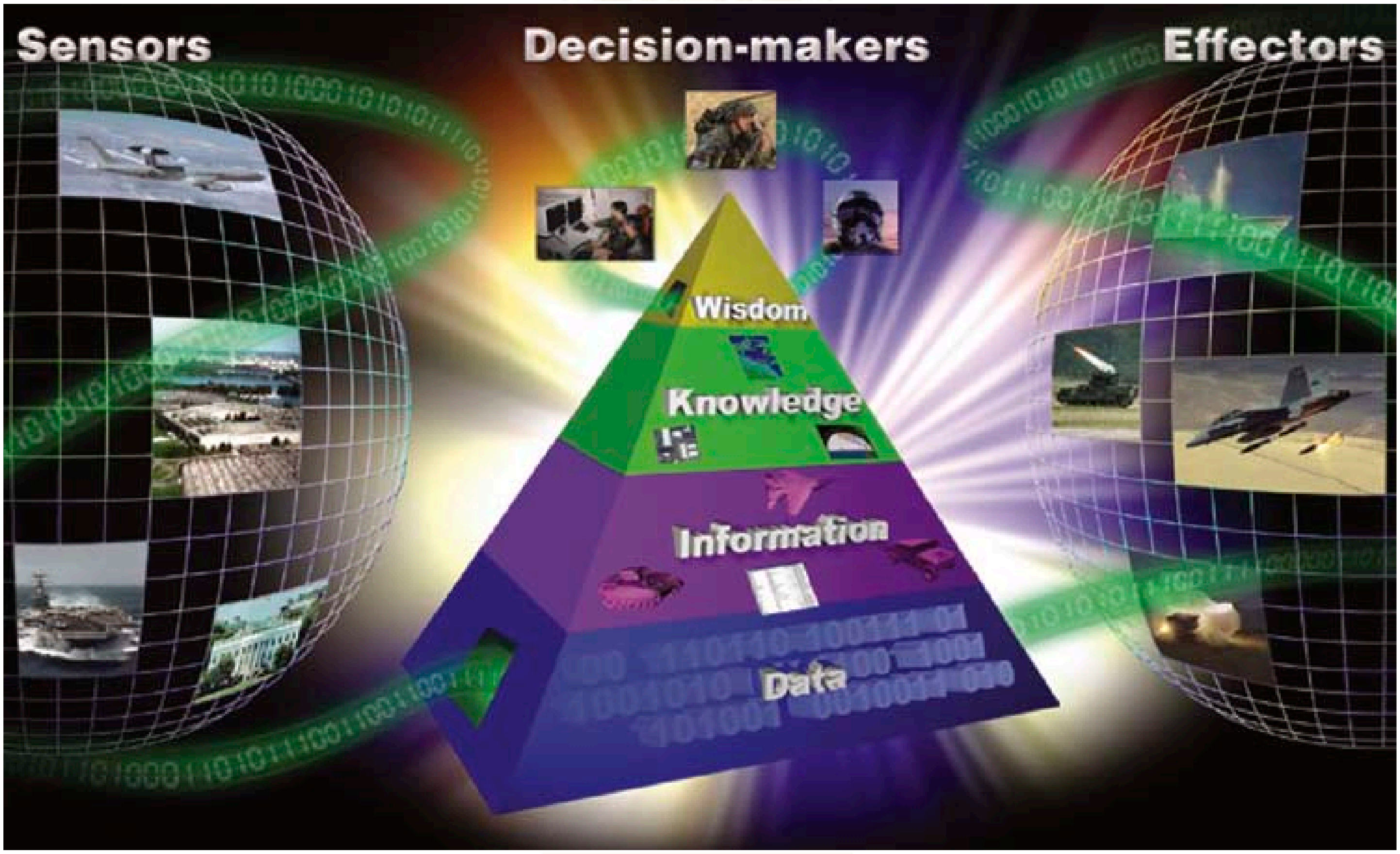
Hanscom Dialing:
Comm'l: 781-377-XXXX
DSN: 478-XXXX

Lt Col Curtis Harvey
Lt Col Robert Pagoni
CFACC
AFC2ISRC/OL-A
Ext. 9350
curtis.harvey@hanscom.af.mil
robert.pagoni@hanscom.af.mil

Capt Jesse Jaramillo
Site Manager
EISG/XR, Ext. 1160
jesse.jaramillo@hanscom.af.mil

Mr. Ronald Goodner
Site Coordinator
& Public Affairs
EISG/XR, Ext. 6397
ron.goodner.ctr@hanscom.af.mil

NET CENTRIC OPERATIONS: The Driving Operational Concept



ity to integrate its command and control, intelligence, surveillance, and reconnaissance (C4ISR) systems--the C2 Enterprise. Integrated C4ISR capabilities will provide an asymmetric force advantage and enable the development of network-centric warfare. Today ESC is integrating systems within the Enterprise to eliminate “stovepipes” and to ensure that warfighters have the capabilities they need to achieve their objectives.

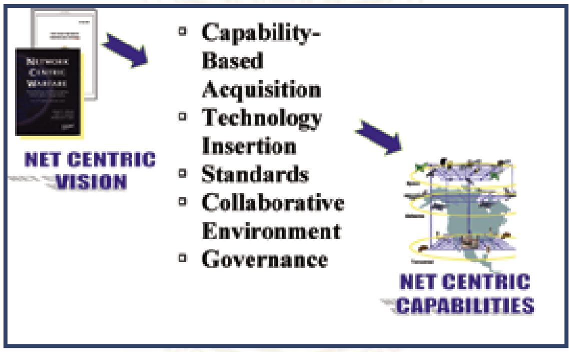
Integrating today’s battlefield and combat environment is quickly transitioning system-to-system (“stovepipe”) integration, to enterprise integration to provide net-centric capability. We are transforming the battlespace; creating a new paradigm where net-centricity is an essential information-centric warfighting capability.

ENTERPRISE INTEGRATION SYSTEMS GROUP

The Enterprise Integration Systems Group was created within the Network Centric Operations & Integration System Wing (NCSW) subordinate to the ESC. Its mission is to lead integration, development, certification, deployment and sustainment of Air Force, Joint, and Coalition C4ISR combat capabilities. Our purpose is to identify technology opportunities to improve C4ISR; provide an integrated environment for examining innovative aerospace operational concepts; and to ensure C4ISR products are fully compatible and interoperable. During CWID 2006, Hanscom AFB hosts the Coalition Force Air Component Commander (CFACC). Key Coalition Air Operations Center (CAOC) leadership positions are simulated to facilitate the CWID assessment process and are located in the C4ISR Enterprise Integration Facility (CEIF). USAF personnel and Coalition partners are role players in the Combat Plans and Combat Operations cells of the CAOC. Planners prepare the Air Tasking Order (ATO)/Airspace Control Order (ACO). Together with the Master Scenar-

Network Engineering
Mr. Bill Page
EISG/XR, Ext. 8458
william.page.ctr@hanscom.af.mil

Systems Engineering
Mr. Bob Gee
EISG/ET, Ext. 6666
robert.gee.ctr@hanscom.af.mil



- Capability-Based Acquisition
- Technology Insertion
- Standards
- Collaborative Environment
- Governance

io Events List (MSEL), the ATO provides the backdrop to assess enhanced capability provided to the warfighter by the various Interoperability Trials (ITs).

In addition, ESC hosts ITs in support of U.S. Northern Command (USNORTHCOM) to evaluate emerging technologies for local and Federal agencies involved in Homeland Security and Homeland Defense (HLS/HLD).

Ultimately, ESC champions the concepts and capabilities of Net-Centricity to U.S., NATO, Coalition, and HLS/HLD forces.

NET CENTRIC OPERATIONS

The Office of Force Transformation (OFT) in the Department of Defense has identified network-centric operations (NCO) as the core of military transformation. At the most fundamental level, NCO generates an information advantage and translates it into a competitive advantage.

This approach to the conduct of warfare derives its synergy from the effective linking or networking of the warfighting enterprise.

NCO is characterized by decision makers, geographically dispersed but connected by digital communications links, that enables them to plan and execute complex operations. NCO considers the commander's intent in a self-synchronized manner during high tempo operations.

THE VISION

The vision is to have a Global Information Grid (GIG), in which all C2 assets are connected. The GIG will contain an infrastructure that allows platforms to be connected and to seamlessly share information. Regardless of what the conflict is or where it is, we need to be dynamic, flexible, and able to adapt to any situation and manage the information on the network. In the final analysis, the best information is available to the decision makers in a timely manner.

The GIG is a combination of assets that can communicate and share information to achieve the proper effects. The GIG requires an architecture that is flexible enough to allow continued communications and exchanges, regardless of the time, place, number of conflicts, military objectives, or situation.

The joint community wants to build a global C2 capability based on Capability Acquisition strategy that the Air Force is defining. An example is the Network Enabled Command Capability (NECC) system for information technology that will enable decision superiority via advanced collaborative information sharing achieved through vertical and horizontal interoperability.

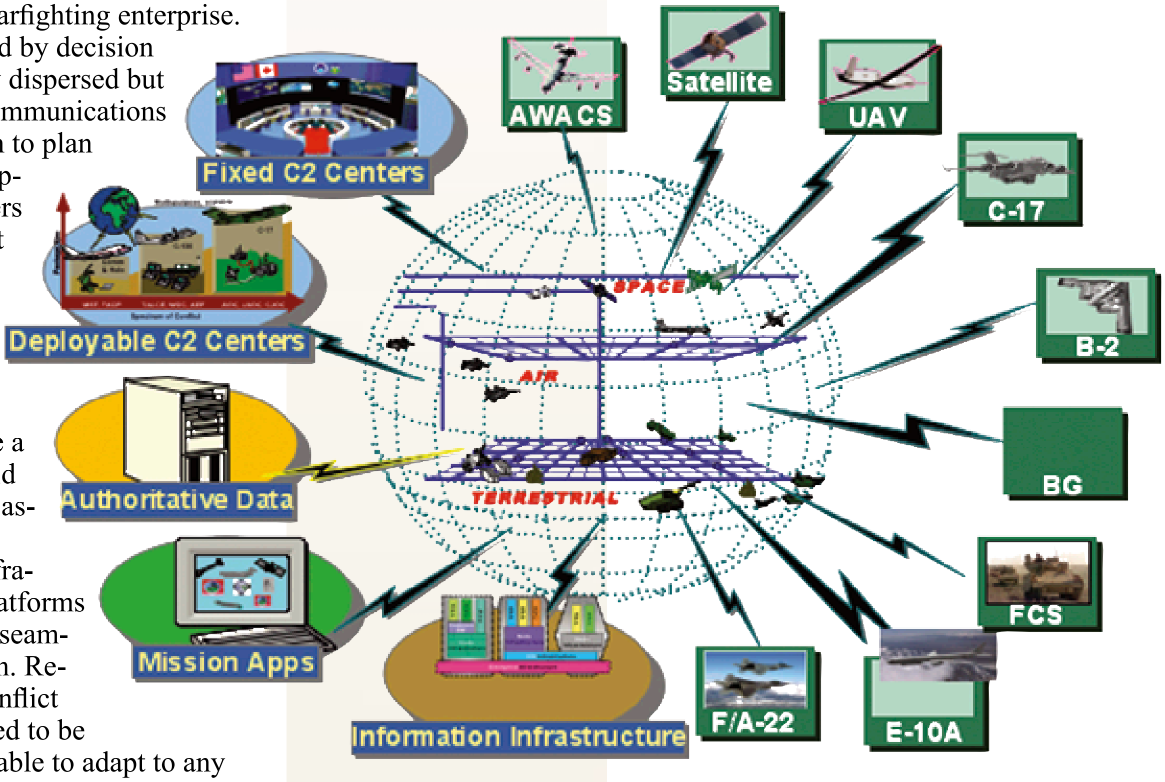
REQUIRED ACQUISITION INNOVATION

The acquisition community must implement a variety of new processes and procedures to achieve the transformation to net-centricity.

Scenario & MSEL Development
SSgt J.T. Kristant
EISG/XR, Ext. 6008
john.kristant@hanscom.af.mil

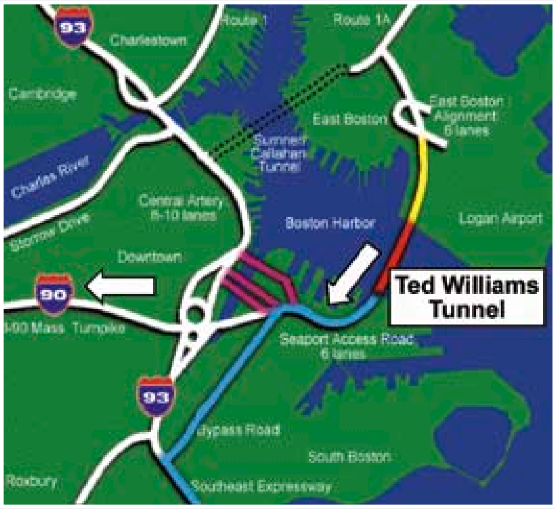
Network Certification & Accreditation
Mr. Larry Barrows, EISG/ET
802-859-0341
larry.barrows.ctr@hanscom.af.mil

COMSEC Custodian
Mr. John McElhinney
EISG/XR, Ext. 5535
john.mcelhinney.ctr@hanscom.af.mil



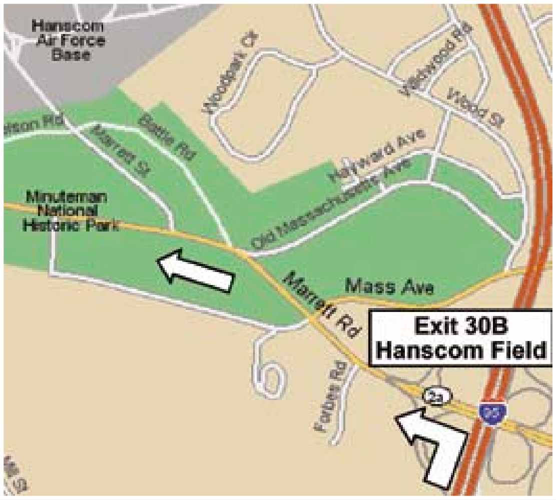
THE VISION: An Integrated Enterprise

Directions to Hanscom Air Force Base



LOGAN INTERNATIONAL AIRPORT/BOSTON

- ■ Upon leaving Logan, follow signs to I-90 West/ Ted Williams Tunnel
- ■ After the Tunnel, keep following I-90 West toward Exit 15
- ■ Take Exit 15 to access I-95/Rt 128 North
- ■ Continue on I-95 North to Exit 30
- ■ Take Exit 30 and continue on to Exit 30B, Hanscom Field/Concord
- ■ Take Rt 2A West (Marrett Rd) and follow signs to Hanscom Field/ AFB
- ■ Register your vehicle at the Visitor Center (Vandenberg Gate)



VANDENBERG GATE

VISITOR CENTER HOURS: 5:00 AM – 10:00 PM

A cross-service effort between ESC and the Navy (the Program Executive Office for C4I and Space), developed the Net-Centric Enterprise Solutions for Interoperability (NESI) concept to provide a framework, the implementation guidance, technical criteria, and reusable software components that facilitate the design, development, and use of information systems for the NCO environment.

This process is accomplished through a Strategic Technical Plan and a set of standards and implementations that allow programs to build their information in ways that conform to the standards. NESI has been provided to other Department of Defense (DoD) services and agencies for potential adoption. The overall goal is to provide common, cross-service guidance in basic terms for the program managers and developers of net-centric solutions. All users can tie into a common communication network. Depending on where they are in each of these nodes they’ll have access to any information on the net that is built on open standards. Instead of dictating what technology is built and how it is built, it’s better to build it into the node. Whatever anyone makes available on the network must be accessible to everyone in an open standard that everyone understands.

The framework allows programs to build their information so it can be discoverable and easily transmitted and received across the different nodes within the theater. This is enterprise integration. ESC is developing sound policies, guidance, and direction to ensure we effectively use scarce resources to achieve the desired value and benefits inherent in enterprise integration.

FOREIGN VISITOR CONTACT

Mr. Clark Foreid
EISG/XR, Ext 4199
FAX: Ext. 2200
clark.foreid@hanscom.af.mil

VISIT REQUEST & SHIPPING ADDRESS

EISG/CO

Attn: Mr. Gil Ynostroza
15 Eglin Street, Bldg 1607
Hanscom AFB, MA 01731
Ext. 2152, Fax Ext. 2200
gil.ynostroza@hanscom.af.mil

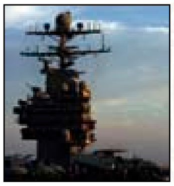
VANDENBERG GATE VISITOR CENTER

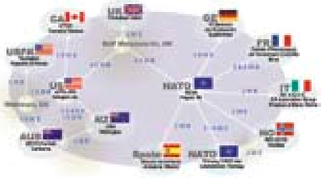
HOURS
6:00 AM – 10:00 PM

Additional info about Hanscom AFB or ESC may be found at:
http://esc.hanscom.af.mil

Trials at Hanscom Air Force Base

IT01.01	Northern European Command - C2 Information System (NEC CCIS)
IT01.15	C4I Defense
IT01.28	Mission Management Suite (MMS)
IT02.21	The Multi National Coalition Security System (MNCSS)
IT02.25	Distributed Common Ground System (DCGS)
IT03.09	Document Access Servelet (DAS)





NATIONAL SECURITY AGENCY, FORT MEADE, MD.

Finding Vulnerable Back Doors

November 7, 2001, the Senior Management Group of the Joint Warrior Interoperability Demonstration (JWID, now CWID) program commissioned NSA to perform a security assessment of interoperability trials that participate in the event.

NSA's approach is consistent with the National Security for Telecommunications and Information Systems Security Policy "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products" and the National Information Assurance Program (NIAP). Security assessment results may be input to security design (e.g. NIAP validation) and the Certification and Accreditation (C&A) processes (e.g. DITSCAP, NIACAP).

SECURITY ASSESSMENT APPROACH

NSA models the "security environment" in terms of "threats" (or threat events) anticipated for an operational deployment, policy statements that apply, and assumptions about how trial capabilities will be used. Respective trials are assessed against this model of the security environment to determine how the capability counters each identified threat, and enforces each identified policy, consistent with assumptions regarding how the capability will be used. Mapping between the warfighter's security environment and the trial's specific security countermeasures, NSA performs a security protection coverage and exposure analysis. Coverage analysis identifies threats specifically addressed by the demoonstration or trial. Exposure analysis identifies threats handled by the environment where the capability is deployed, representing actual "security benefits."

RESULTS OF SECURITY ASSESSMENT

2006 is the fifth year NSA has performed Security Assessments with CWID (formerly known as JWID). NSA continues to collect data on the effectiveness of the assessment. "Gold Nuggets" from JWID 2001-2002 did commit to having security protection implemented within their products validated through the NIAP process. One vendor was successful taking two products through the NIAP process: BMC Software PATROL® was certified by NIAP September 30, 2002; and PATROL® Perform/Predict was certified April 8, 2002. Other JWID/CWID vendors reported enhancements to the security of their products, but have not yet validated them with a NIAP Accredited Laboratory.

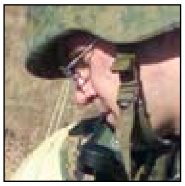
NSA performed 23 Security Assessments for 2005. Criteria determining which trials will be assessed in CWID is based on the NSTISSP No.11, which targets IA and IA-enabled products. The Security Assessment report that is generated through the CWID Security Assessment Process can be used directly by vendors to create Security Target documentation, or by security practitioners to create a Protection Profile for their respective IA needs. The report also identifies specific security coverage areas and protection exposures that should be addressed as part of a formal C&A of every operational deployment of these capabilities.

CONTACT

Lt. Col. Todd Sasaki
tmsasak@missi.ncsc.mil

ADDRESS

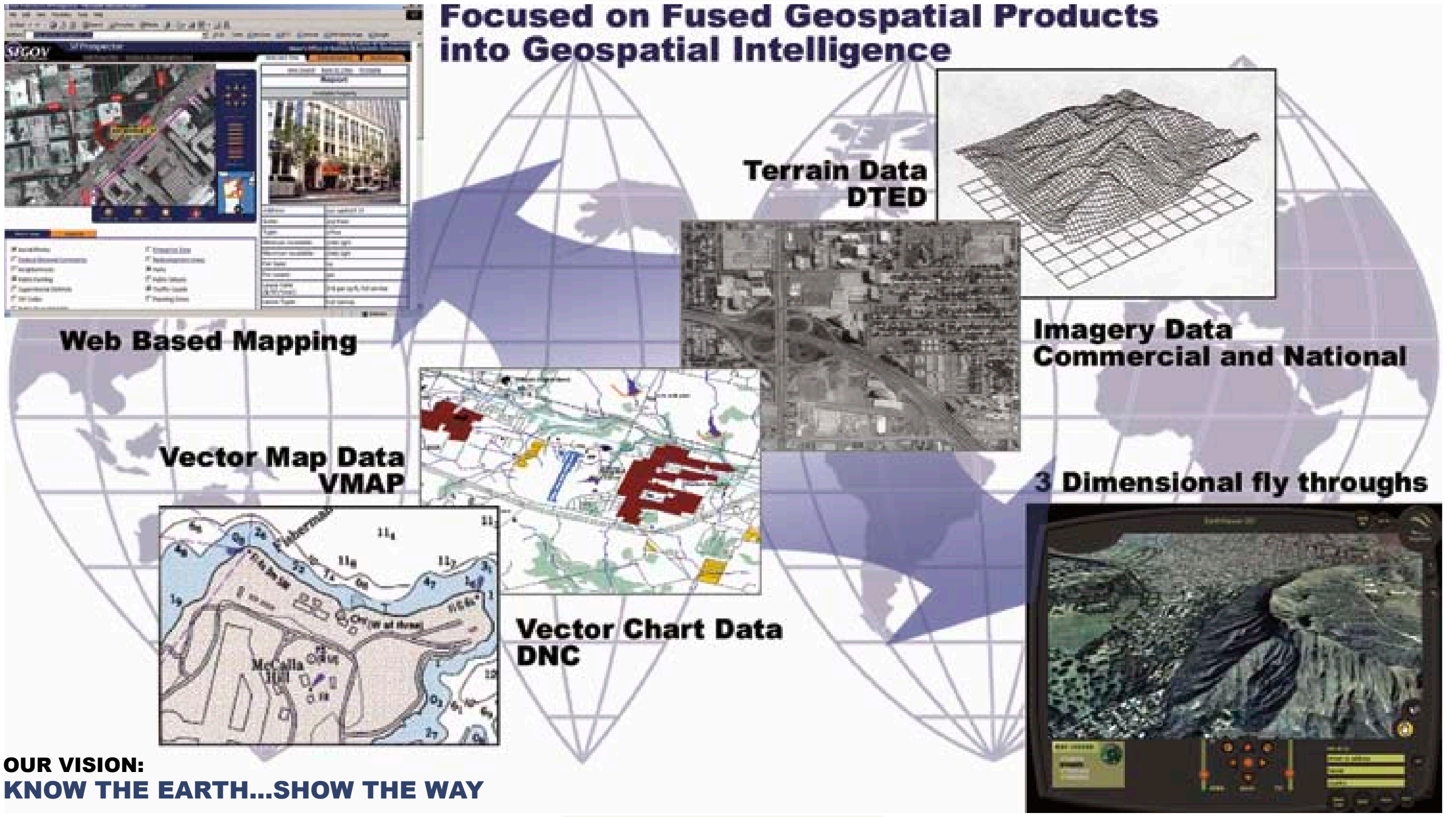
NSA
9800 Savage Rd.
Ft. Meade, MD 20755



NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

Supplying the Space-Eye View

The National Geospatial-Intelligence Agency (NGA) provides timely, relevant, and accurate Geospatial Intelligence (GI) in support of national security. GI in all its forms, and from whatever source—imagery, imagery intelligence, and geospatial data and information—ensures the knowledge foundation for planning, decision, and action. NGA provides easy access to GI databases for stakeholders. The agency creates tailored, customer-specific GI, analytic services, and solutions. NGA, in partnership with coalition GI agencies, is proud to provide GI and other information services for CWID 2006.



OUR VISION:

KNOW THE EARTH...SHOW THE WAY

OUR CORE VALUES:

- In NGA, we are committed to...

CUSTOMERS

- Both as a National Intelligence and a Combat Support Agency

PEOPLE

- Their personal integrity, professionalism, growth, leadership, and accountability

CULTURE

- Our diversity, teamwork, creativity, risk-taking, and mutual trust and respect

...EXCELLENCE IN ALL WE DO

POINTS OF CONTACT

Mark Thomas
mark.k.thomas@nga.mil
703.735.3599

Don Talada
taladad@nga.mil
703.735.3524

ADDRESS

NGA
4600 Sangamore Rd.
Bethesda, MD 20816-5003

JOINT INTEROPERABILITY TEST COMMAND

Focusing on Interoperability

As tasked in Chairman of the Joint Chiefs of Staff Instruction 6260.01, JITC supports CWID in the following ways:

SENIOR MANAGEMENT GROUP

JITC provides a non-voting representative to the CWID SMG to advise the SMG on interoperability issues and challenges.

ASSESSMENT WORKING GROUP

As Chairperson of the AWG, JITC ensures that assessments performed by the Technical, Warfighter Utility and Information Assurance Assessment Teams compliment each other and provide an overall assessment of all aspects of a trial. The AWG Chair also interfaces directly with all other CWID Working Groups on matters related to the assessment of the participating trials.

TECHNICAL ASSESSMENT APPROACH

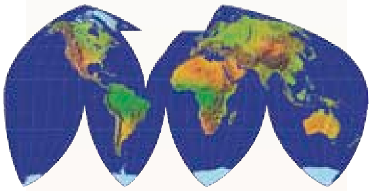
In addition to chairing the AWG, JITC performs Technical Assessments. During CWID execution, JITC assesses and documents interoperability of selected trials by observing pre-determined events (information exchanges) executed against a documented set of requirements at each primary demonstration site. For those trials that do not have formal requirements documents, JITC works with each trial's representative to define requirements for CWID. Requirements focus on details related to data exchanges between the trial and CWID core services or other CWID Interoperability Trials. Details include attributes such as ports and/or protocols used, data or media formats, and data type. Details also define: what information is exchanged; who exchanges the information and who receives the information; why the information is necessary; and how the exchanges take place (physical path). JITC coordinates with each trial assessed to document results of data transfers and information exchanges, ensureing data transferred during the exchange is processed correctly by the receiving system.

INTEROPERABILITY RESULTS

Following execution, JITC analysts review the results of each trial's data transfers demonstrated during execution. JITC documents, in the WISE Interoperability Collection Assessment Tool (WICAT), the successes and any problems encountered during data transfers, and the ability of the end user to process the data exchanged. Once all data has been input and consolidated, JITC passes this information to the CWID Joint Management Office (JMO) in the form of a database that provides a "snapshot view" of the interoperability status of each trial assessed by JITC. In addition, JITC provides the CWID JMO a narrative summary of the WICAT database that further defines trials in the areas of hardware and software configuration and connectivity to the network for inclusion in the CWID Final Report. All data that JITC collects on Information Technology (IT) and National Security System (NSS) trials during the CWID process can be carried forward and applied toward an Interoperability Certification.

INFORMATION ASSURANCE

In its role as an Operational Test Agency (OTA) for the Director, Operational Test and Evaluation (DOT&E), JITC supports CWID by augmenting the NSA in the preparation and conduct of Information Assurance Assessments performed on selected ITs. If required, JITC can support the staff assigned to the National Information Assurance Team (NIAT) during CWID execution.



CONTACT

Jeff Phipps
(301) 744-2883
(DSN) 354-2883
jeff.phipps@disa.mil

http://jitc.fhu.disa.mil/